PRODUCT BULLETIN

PULSE CONNECT SECURE, PULSE POLICY SECURE AND PULSE CLIENT UPDATES FOR 9.1R5

Bulletin Date

April 2020

Applicable to All

Regions Effective

Change Date

April 2020

Introduction

Today's digital era is challenging workforce productivity, from the 9-to-5 workdays to means of accessing and digesting data. More importantly, access to data and applications across different mediums, mobile to cloud, are redefining traditional IT processes and policies. Pulse Secure has made it easier to secure your data center, provide mobile access and enable new cloud services with our integrated Secure Access Solution. This Product Bulletin describes new features and functions available in the 9.1R5 release of Pulse Connect Secure, Pulse Policy Secure, and the Pulse Secure Desktop Client.

These new releases from Pulse Secure enable network administrators to expand their secure access solution support for network performance and security.

This release focuses on customer requirements, SBR to PPS migration use cases, support for SDP enabled client on macOS and FQDN based Split tunneling improvements. Backup and recovery support for profilers.

What's New

Common Features for Pulse Connect Secure and Pulse Policy Secure

Key Feature	Benefit

• Password management for OpenLDAP	• LDAP-based password management works with generic LDAP servers such as OpenLDAP
	  ◦ Users to change the password for initial login.
	  ◦ Users to change password on expiry.
	  ◦ Users can change password at anytime through end-user portal page.

• Change default gateway on cloud installation	• In PCS hosted on a cloud environment, it is now possible to edit default gateway configuration from UI.
• License server with Active-Active cluster	• Administrators can: • Create license server with Active/Active cluster on virtual/cloud and hardware platforms. • Please all different type of licenses to license clients from any node of active-active cluster. • Surrender/recall licenses from any node of active-active cluster.
• Host Checker policy to detect hard disk Encryption in progress	Host Checker policy to allow detection of hard drive encryption in progress.

Pulse Connect Secure 9.1R5

For detailed information on SDP, refer to the following SDP documents on https://www.pulsesecure.net/techpubs.

- SDP Release Notes
- SDP Supported Platforms Guide
- SDP Getting Started Guide
- SDP Deployment Guide

The following table lists the non-SDP features for Pulse Connect Secure 9.1R5.

Highlighted Features in this Release

Key Feature	Benefit
• Terraform template support for AWS and Azure	• PCS provides Terraform template support for AWS and Azure. These templates are release-independent and are available as part of the Pulse Secure download page.

• MSSP Reporting Enhancements	• It is now possible to extract any specific license client/cluster report through REST API. Enhancements include:
	  ◦ Cluster-wise view in the license report.
	  ◦ License report in JSON format through REST.
	• Options to get cluster/client/period sub-section of the granular report through REST.

• SSLDump for VLAN	• In this release, SSLDump utility supports VLAN. Admins can use this tool for debugging / data collection purpose.
• Rewriter Enhancements	• Rewriter engine provides framework support of Ember and Angular js.
• Microsoft Intune MDM integration	• In this release, the Pulse Secure device access management framework supports integration with Microsoft Intune.

Cloud Secure Specific Features in Pulse Connect Secure 9.1R5

Highlighted Features in this Release

Key Feature	Benefit
• Location based Conditional Access	• Conditional Access feature for Cloud Secure now provides a mechanism to enforce access control policies based on location parameters by defining policies for applications.

Pulse Policy Secure and Profiler 9.1R5

Highlighted Features in this Release

Key Feature	Benefit
SNMP policy enforcement (Alcatel-Lucent, Huawei, Arista)	SNMP policy enforcement is now supported on Alcatel-Lucent, Huawei and Arista switches.
Pulse Policy Secure on Amazon Web Services (AWS)	Provides NAC services (802.1x, MAC Auth, L3 Firewall Enforcement) using PPS deployed on Amazon Web Services (AWS) cloud.
McAfee ePolicy Orchestrator (ePO) integration	Pulse Policy Secure (PPS) integration with the McAfee ePolicy Orchestrator (ePO) provides complete visibility of network endpoints and provide end to end network security. The PPS integration with McAfee ePO allows Admin to perform user access control based on alerts received from the McAfee ePO.
Splunk syslog add-on and Dashboard app	Splunk application for PPS uses the indexed data to render various charts and to show useful information on dashboard. The Pulse Secure App for Splunk allows you to view PPS data in a dedicated, customizable Splunk dashboard. This bidirectional interaction with Splunk allows security managers to quickly monitor the current operational/security posture.
SBR to PPS migration	SBR configurations can be migrated to PPS using wizard option.
ECC certificate support for Juniper SRX firewall.	PPS now supports Elliptic Curve Cryptography (ECC) certificate communication/connection for SRX firewall.
IPv6 Support for Syslog, NTP and Log Archive	• PPS now supports sending syslog messages to a syslog server using IPv6 address. Time synchronization using NTP server is now supported with IPv6 address. PPS also supports transferring archived PPS logs using FTP and SCP over IPv6 network.
MSSQL support on PPS with external DB	• PPS supports MSSQL as external Auth server for 802.1X and Layer 3 authentication.
Profiler	
Backup and Recovery, and Disaster management	Profiler deployments provides backup mechanism for enhanced disaster management using the primary and secondary profiler setup.

Pulse Secure Desktop Client 9.1R5

For detailed information on SDP, refer to the following SDP documents on https://www.pulsesecure.net/techpubs.

- SDP Release Notes
- SDP Supported Platforms Guide
- SDP Getting Started Guide
- SDP Deployment Guide

The following table lists the non-SDP features for Pulse Desktop Client 9.1R5.

Highlighted Features in this Release

Key Feature	Benefit
• PSAM session window	• This feature allows the PSAM users to view the active session information of the configured applications and destinations.
• Security Enhancement to support HTTPOnly cookie	• Added support to handle the HTTPOnly session cookies in pulse client as part of security enhancement.
• Disabling JNPRNS via Advance Client configuration	The feature runs a script/workflow to disable JNPRNS driver every time the user establishes a VPN connection and prevents reattaching of JNPRNS driver on restart. This process results in slight increase in time taken for establishing the VPN connection.

Learn More

Resources

- Pulse Connect Secure datasheet
- Pulse Policy Secure datasheet
- Pulse Cloud Secure product brief

www.pulsesecure.net

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize Pulse Secure's Virtual Private Network (VPN), Network Access Control (NAC) and mobile security products to enable secure end-user mobility in their organizations. Pulse Secure's mission is to provide integrated enterprise system solutions that empower business productivity through seamless mobility.

Corporate and Sales Headquarters Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net